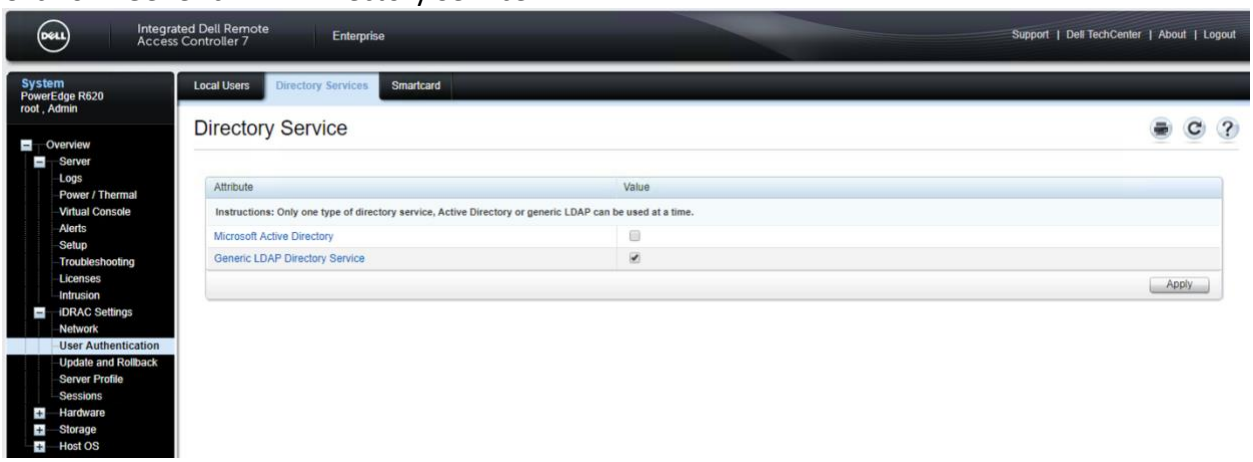
iDrac Configuration Guide

1) Configure Directory Services for iDrac.

In the case of PUA. iDrac User Interface Must be point “back” to an LDAP VIP on the PUA system for Authentication.

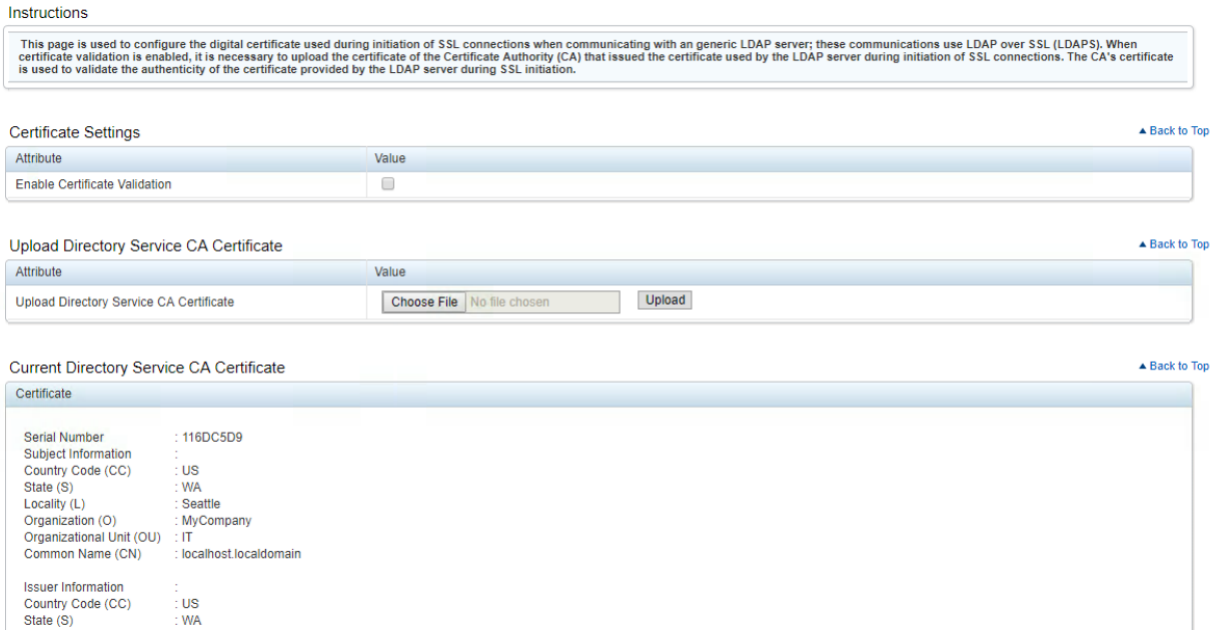
Select System/User Authentication/Directory Services

Click on “Generic LDAP Directory Service”



Select the “Configure Generic LDAP” button..

Upload the Directory Service CA Certificate – in this case the generic F5 self-signed CA Certificate was selected as this was CA Certificate that was associated with the “636” or LDAPS VIP.



Step2 of 3

These are the settings that worked in our case.. depending up on the ultimate Directory these setting may be different. Our “ultimate” back end directory was a Windows Directory.

Enable Generic LDAP “checked”
Use Distinguished Name
LDAP Server Address:- IP of LDAPS VIP for PUA
LDAP Server PORT:- 636.. could be configured to be a different port if the VIP was listening on something other than default.
Bind DN: Whatever you BIND DN would be for your directory… in our case it was cn=Administrator,cn=Users,dc=afspc,dc=local
Attribute of User Login :- sAMAccountName
Attribute of Group Membership:- member

Step 2 of 3

Instructions

This page is used to configure location information about generic LDAP servers and user accounts.

Common Settings ▲ Back to To

Attribute	Value
Enable Generic LDAP	☑
Use Distinguished Name to Search Group Membership *(if unchecked, username will be used)*	☑
LDAP Server Address *(FQDN or IP, must match the server certificate if certificate validation is enabled)*	10.246.49.218
LDAP Server Port *(Only SSL port is supported)*	636
Bind DN *(required if anonymous bind is not allowed)*	cn=Administrator,cn=Users,dc=afspc,dc=local
Update Bind Password	☐
Bind Password *(required if anonymous bind is not allowed)*	
Base DN to Search *(e.g. dc=example,dc=com, required)*	cn=Users,dc=afspc,dc=local
Attribute of User Login *(e.g. uid)*	sAMAccountName
Attribute of Group Membership *(e.g. member or uniquemember)*	member
Search Filter *(e.g. objectclass=*, optional)*	

Create a Role Group.

Your configuration may be different but each role group will have a role within the iDrac which will have certain group privileges associated with it.

In our case we create a single “Administrator” role group that was associated with a specific group in the Windows Active Directory Server

Step 3a of 3

Instructions

This page is used to configure the privilege groups used to authorize users. When Generic LDAP is enabled, it is necessary to configure Role Group(s) used that specify authorization policy for iDRAC users.

Group Settings ▲ Back to Top

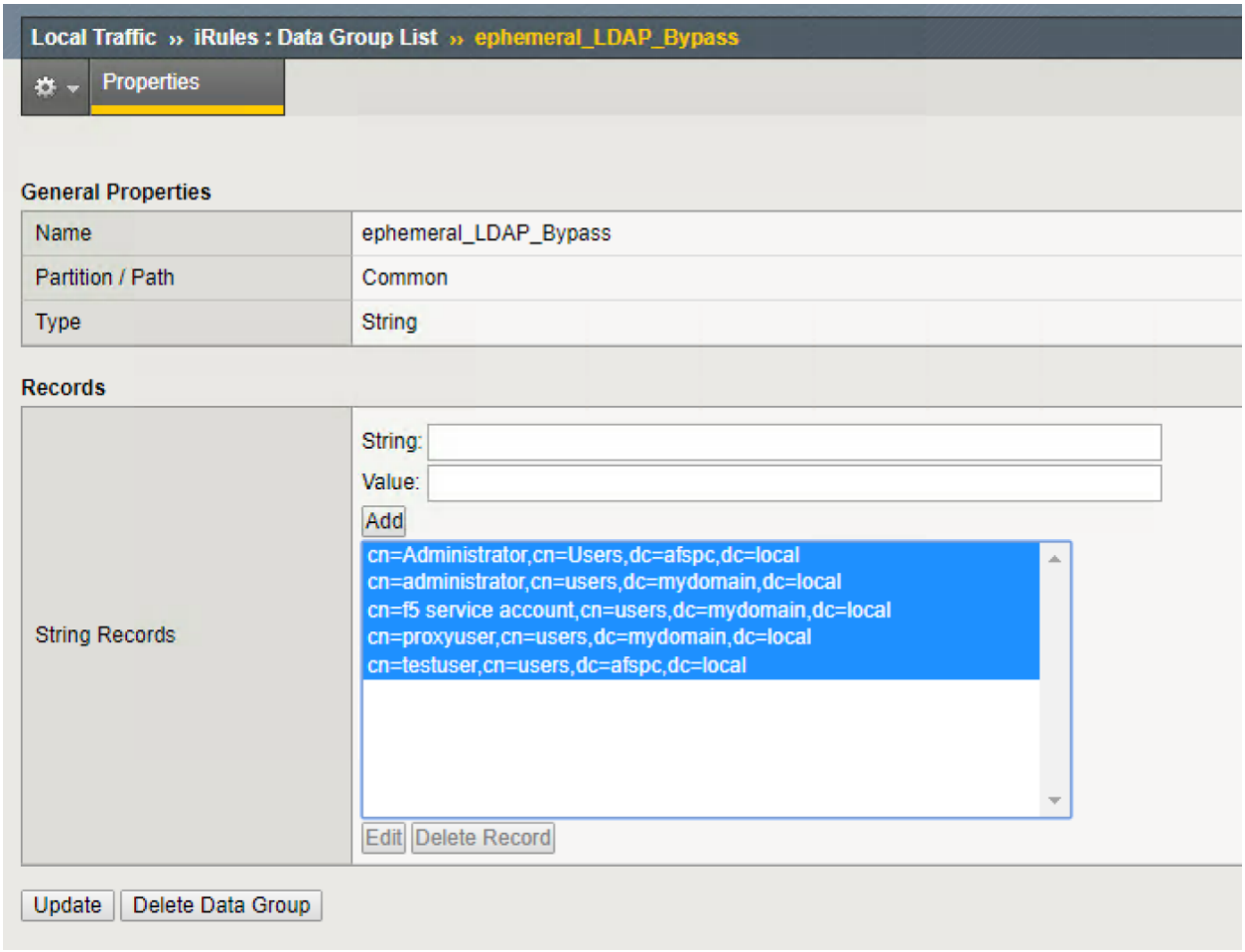
Role Groups	Group DN	Group Privilege
Role Group 1	CN=Administrators,CN=Builtin,DC=afspc,DC=local	Administrator
Role Group 2		None
Role Group 3		None
Role Group 4		None
Role Group 5		None

Click Finish..

Select the “Test Settings Button”

Then enter a username and password of an active directory user. If the test passes then you can continue with the F5 Configuration.

Note: The DN that username translates to must be in the ephemeral_LDAP_Bypass data-group. Otherwise the PUA system will intercept the authentication and generate an ephemeral credential and the authentication will fail. This data group is under iRules/DataGroup List



2) Create Portal Access Resource for iDrac

In the APM menu select Connectivity / VPN : Portal Access : Portal Access Lists

Name: Your choice “iDrac” for example
Leave Patching to be default.
Application URI: Needs to be the IP or hostname of the iDrac Server

General Properties

Name	iDrac
Partition / Path	Common
Description	
ACL Order	2

Configuration: Advanced

Match Case For Paths	Yes
Patching	Type Full Patching HTML Patching JavaScript Patching CSS Patching Flash Patching Java Patching
Publish on Webtop	Enable
Link Type	Application URI
Application URI	https://10.253.20.215
Proxy Host	
Proxy Port	0

Customization Settings for English

Language	English
Caption	iDrac
Detailed Description	
Image	Choose File No file chosen View/Hide Restore Default

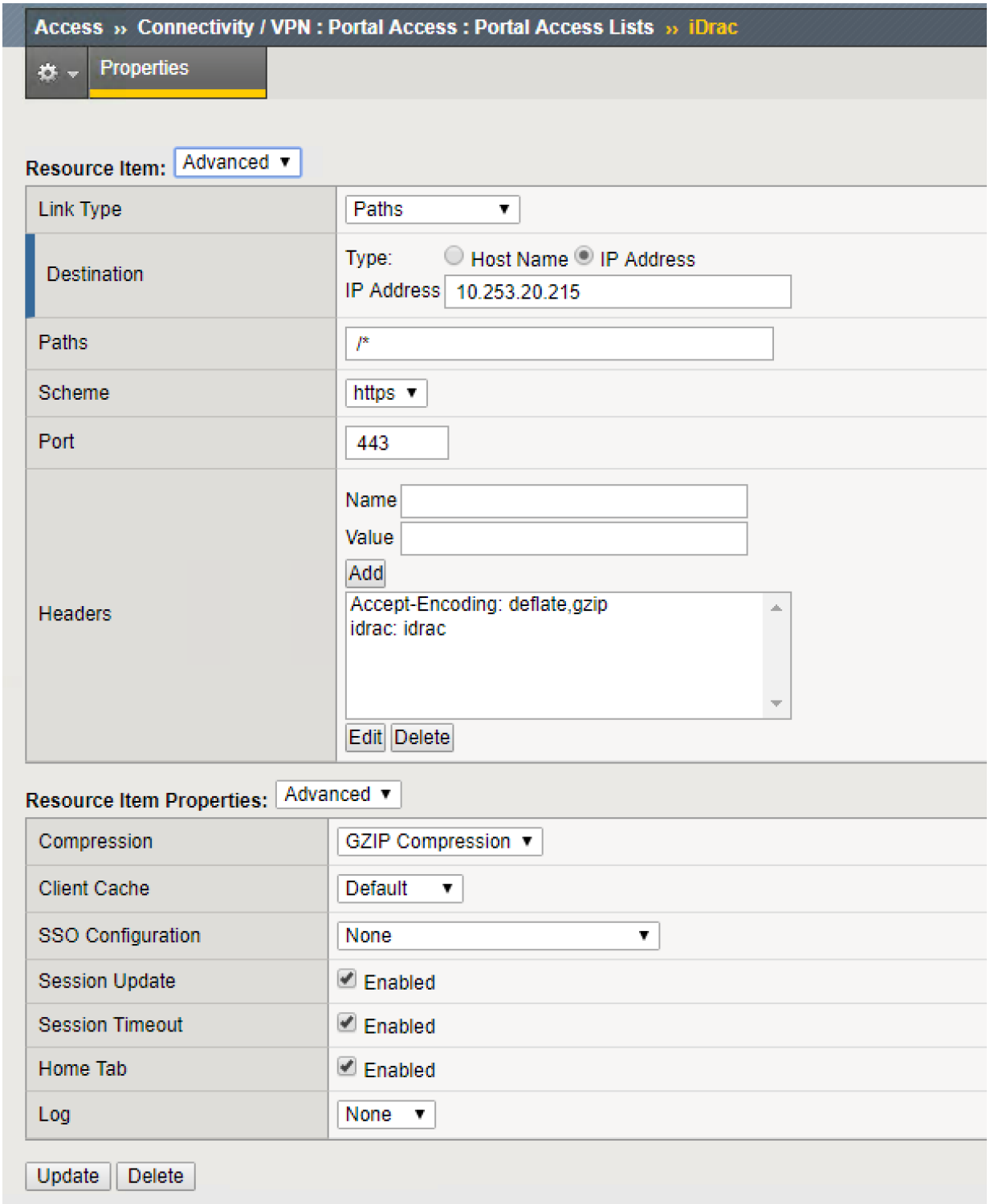
Update Delete

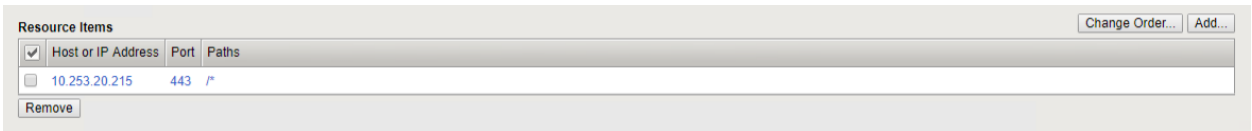
3) Create a Resource Item withing the portal Access Resource.

For resource type use the IP Address.
For Link Type Select “Paths”
For the Paths Entry Field type /*
Scheme = https
For Headers Add

Name: Accept-Encoding
Value:deflate, gzip

Name: idrac
Vlaue: idrac


Access » Connectivity / VPN : Portal Access : Portal Access Lists » iDrac
Properties
Resource Item: Advanced
Link Type
Paths
Destination
Type: Host Name IP Address
IP Address 10.253.20.215
Paths
/*
Scheme
https
Port
443
Headers
Name
Value
Add
Accept-Encoding: deflate,gzip
idrac: idrac
Edit Delete
Resource Item Properties: Advanced
Compression
GZIP Compression
Client Cache
Default
SSO Configuration
None
Session Update
Enabled
Session Timeout
Enabled
Home Tab
Enabled
Log
None
Update Delete


Resource Items
Change Order... Add...
Host or IP Address Port Paths
10.253.20.215 443 /*
Remove

4) Apply the iDrac iRule to the VIP .. for example a “PUA Webtop” VIP

Note: This iRule depends on session variables existing in the APM policy.

session.logon.last.username
session.custom.ephemeral.last.password_sso

Insert iRule Below

```
when REWRITE_REQUEST_DONE {


   #check for the existence of the correct uri
   if { [HTTP::uri] ends_with "/login.html" || [HTTP::header exists idrac] } {



      set workaround 1
      REWRITE::post_process 1

   } elseif { [info exists workaround] } {
      unset workaround
   }
}

when REWRITE_RESPONSE_DONE {
   if { [info exists workaround] } {
      unset workaround
      set location [string last "</body>" [REWRITE::payload]]
      if { $location > 0 && \
           $location < [expr {[REWRITE::payload length] - 5}]
      } {
                           set username [ACCESS::session data get session.logon.last.username]
                           set password [ACCESS::session data get
session.custom.ephemeral.last.password_sso]
                           set newstring "<script>
var checkExist = setInterval(function() {
  if (document.body.contains(document.getElementById(\"user\"))) {
    clearInterval(checkExist);



           document.getElementById(\"user\").value = \"$username\";
```

```
            document.getElementById(\"password\").value = \"$password\";
            frmSubmit();


    }
}, 2000); // check every 2 seconds. Can be adjusted if timing is an issue.
</script>"

                                REWRITE::payload replace $location 0 $newstring
        }
        unset location
    }
}
```

5) You can then associate the portal access resource item with the Webtop Policy.

- Click Access/Profiles
- Click “Edit” under Per-Session Policy
- Select the Webtop. This will be associated with an “Advanced Resource Assign Webtop Item”
- Then Select the Add/Delete Button
- Then select the Portal Access Tab
- Then Select the Portal Access webtop Item that you want to display on the webtop… for Example. “Unity”